Experimental quantum key distribution certified by Bell's theorem

Security

By Terra Quantum AG
terraquantum.swiss

2022

Experimental quantum key distribution certified by Bell's theorem

DP Nadlinger, et al.

ABSTRACT

Cryptographic key exchange protocols traditionally rely on computational conjectures such as the hardness of prime factorization[1] to provide security against eavesdropping attacks. Remarkably, quantum key distribution protocols such as the Bennett–Brassard scheme[2] provide information-theoretic security against such attacks, a much stronger form of security unreachable by classical means. However, quantum protocols realized so far are subject to a new class of attacks exploiting a mismatch between the quantum states or measurements implemented and their theoretical modelling, as demonstrated in numerous experiments[3,4,5,6]. Here we present the experimental realization of a complete quantum key distribution protocol immune to these vulnerabilities, following Ekert's pioneering proposal[7] to use entanglement to bound an adversary's information from Bell's theorem[8]. By combining theoretical developments with an improved optical fibre link generating entanglement between two trapped-ion qubits, we obtain 95,628 key bits with device-independent security[9,10,11,12] from 1.5 million Bell pairs created during eight hours of run time. We take steps to ensure that information on the measurement results is inaccessible to an eavesdropper. These measurements are performed without space-like separation. Our result shows that provably secure cryptography under general assumptions is possible with real-world devices, and paves the way for further quantum information applications based on the device-independence principle.

The full article can be found here:
https://www.nature.com/articles/s41586-022-04941-5